State of Connecticut

Enterprise Systems Management Domain

Technical Architecture

January 4, 2001

Version 1.0

TABLE OF CONTENTS

Mission Statement

Enterprise Systems Management Architecture defines the framework for efficient and effective management of the State's computing environment in order to support and enhance the productivity of its automated business systems. The principles in this domain help guide the evaluation, selection, design, construction, and implementation of the domain and its elements.

Introduction and Background

The State's Enterprise Systems Management Architecture is the framework that identifies the requirements for managing and supporting the enterprise-wide technical architecture with emphasis on centrally managing distributed computer solutions at geographically disbursed sites. Resources managed include the systems, databases, applications, networks, and Internet and Intranet components necessary to conduct the automated business functions of the State.

Currently, the State's mainframe computer operations environments utilize comprehensive Enterprise Systems Management disciplines, standards, and tools which are well defined for mainframe computing, and which have a long history of successful use.

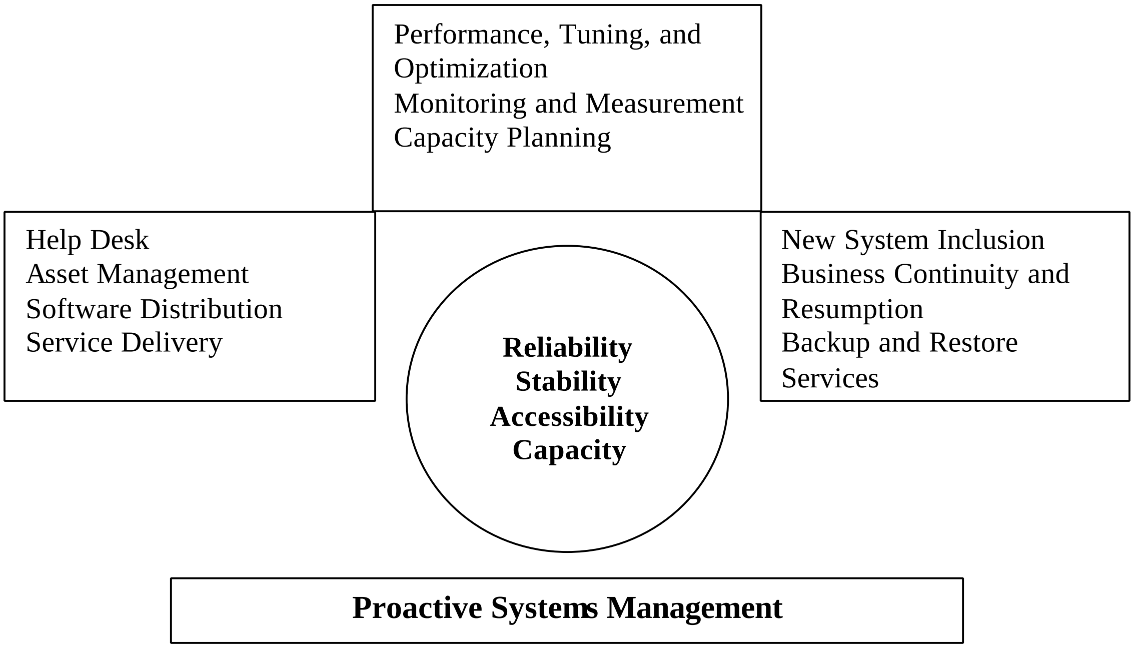
The rapid advances in desktop and local server based computing in recent years have led to a multitude of PC, LAN and WAN configurations deployed locally to meet specific computing needs. User preference for PCs with a GUI interface has led to the transition of mission critical applications from the secure mainframe 'glass house' environment to the less secure workplace. This has greatly increased the complexity and challenges of Enterprise Systems Management for the distributed computing environment. Unlike mainframe computing, which has developed reliable tools and practices over the years, distributed Enterprise Systems Management tools are in the formative stage of their life cycle. Vendors are investing in developing and enhancing their Enterprise Systems Management products. They are building through various means integrated suites of products to manage complex environments, developing relationships with other vendors, and building Enterprise Systems Management functionality into their products. Point product solutions are available for specific distributed functions. However, fully integrated Enterprise Systems Management product suites for the distributed environment have just begun and have yet to achieve full market maturity.

To meet the challenges of the information-processing environment, it is necessary for organizations to transition systems management to the well-designed disciplines found in host-based systems. Standards and procedures are being developed that will support all mission critical client/server applications regardless of where they reside. Enterprise Systems Management applies the appropriate standards, practices, procedures and tools to all types of computing environments. Use of Enterprise Systems Management would enable the State to maximize the use of its information processing resources and enhance the accessibility, timeliness, and quality of service to its citizens.

The existence of a common uniform network (see *Network Domain Technical Architecture*, elsewhere) provides the backbone that permits the State to benefit from the centralized management of certain distributed computing functions. The centralized management techniques, currently used for mainframe applications, create building blocks of skills and experience that can be applied to the distributed information-processing environment.

Mainframe management concepts, including enterprise data, controlled user access, and production disciplines, are effective, reliable and readily adaptable to the distributed computing environment. The Enterprise Systems Management domain seeks to leverage the proven mainframe concepts to develop a framework of practices, technology and tools to support the management of mission critical, distributed client/server applications and technological resources.

In order to be proactive in supporting the computing environment at the State, it is important to manage the capacity, reliability, stability and accessibility of all computing systems. This is accomplished through performance tuning and optimization, monitoring and measuring, adding newly deployed solutions under Enterprise Systems Management and providing disaster recovery, backup and restoration services. It also includes service delivery, in particular the help desk, as well as asset management and software distribution. The figure, below, illustrates these relationships:


Performance, Tuning, and Optimization
Monitoring and Measurement
Capacity Planning
Help Desk
Asset Management
Software Distribution
Service Delivery
Reliability
Stability
Accessibility
Capacity
New System Inclusion
Business Continuity and Resumption
Backup and Restore Services
Proactive Systems Management

Help Desk

The expansion from mainframe host-based systems to distributed systems has dramatically increased the complexity of the State's business and computing environment. Technological advances, including desktops, laptops, LANs, WANs, office automation, Internet, remote virtual office access, decision support systems, and e-mail/groupware, offer many new opportunities for improving the state's business processes and providing increased citizen interaction with government.

However, the variety of new technology options also increases user frustration and heightens demand for quality support. *One of the most important Enterprise Systems Management Architecture components is the* Help Desk. It must be designed as a customer-oriented business driven service center intimately linked with enterprise computing. A strong help desk structure provides the user support necessary to build and sustain a modern computing environment.

The main frame era help desk

Prior to 1990, the traditional help desk existed to support mainframe computing. It was a front-end support organization for mainframe applications. The help desk was part of a larger technical organization geared to support mainframe operations by fixing technical problems onsite. Its focus was reactive. Staff waited for users to call with problems, which were logged and dispatched.

First level help desk employees were trained to perform only the most basic operations (e.g. password resets). When a more complex call was received, the help desk was just a 'pass through' or entry point to obtaining services. A problem was identified and channeled to the appropriate technician, who worked on the defect and fixed it in the centralized data center (i.e., glass house).

The technician fixing the problem had very little, if any contact with the caller. The job objective was to support the mainframe operation, not the user's business. Most help desk positions were entry level. Many help desk applications were simple, non-integrated, home grown problem-recording systems. Operational metrics were collected and were a count of the number and type of calls. This traditional help desk as problem collector and dispatcher many times led to negative user perceptions of the help desk.

Mid 90's help desk

In the early 1990's, the service driven help desk evolved as a response to the increasing complexity of the distributed computing environment. It is focused on user support and driven by the business process. Client/server architectures often times appear easier than the mainframe for the average user to understand and operate; therefore, client/server systems are used more and customer expectations are higher.

However, the many integrated components of client/server systems make it much more difficult for the average user to diagnose and solve his/her own problems. It is unreasonable to expect a customer to determine if the cause of the problem lies in the application, network or hardware and further decide where to seek assistance. A centralized help desk provides a single point of contact, SPOC (one number to call), which automatically routes the service request to the appropriate resource.

The growth of disparate and departmentalized client/server systems has increased the complexities of IT systems management. Is has also changed the way services are delivered and who receives them. The evolution of the help desk into an automated service desk is an outgrowth of IT management’s response to a steady increase in a wide range of user support requests, service delivery issues, and a more complex computing environment.

The modern service driven help desk

The modern help desk is the cornerstone of the enterprise’s virtual computing management infrastructure. The help desk uses technology wisely to expand into a "fully" operational support center. Its mission is to enable productivity. The modern help desk has the following characteristics.

- It is driven by business needs.
- Centers on customer service.
- Is staffed by career professionals.
- Uses state of the art automated tools to record and track user requests for service.
- Builds knowledge bases of solutions to common problems.
- It empowers both support staff and customers.
- Fosters communication by sharing data and transferring requests among geographically disbursed locations.
- It collects and uses sophisticated metrics to avoid problems that reoccur.
- Performs the problem and resolution management functions.
- Integrates with many other support functions including change, service, operations, asset management, training, installation, and maintenance services.
- Uses a process-oriented approach to link business needs with technology management.

The Help Desk component of the Enterprise Systems Management Architecture supports the ability of all help desks in the state to maintain their own help desk database. It also makes it possible to access and share an enterprise-wide database of client, request, and resolution information. This sharing of information enables the state to more efficiently identify and resolve user problems. It builds on and improves the internal efficiencies of departments.

Electronic Software Distribution

Major software rollouts continuously fall six to nine months behind schedule, due to the Herculean task of delivering applications to a distributed enterprise of heterogeneous clients. Currently, most organizations rely on manual software distribution for application rollouts. Although electronic software distribution (ESD) is not a “Silver Bullet” solution, with proper planning ESD will alleviate much of the repetitive “grunt-level” work. In addition, third-party vendors (e.g., McAfee, Novell, Microsoft, Intel, Seagate, Attachmate, Tivoli) have significantly improved ESD functionality in the last 12 months with: rollback capabilities, network bandwidth control, and ODBC back-end databases.

Packaging

Packaging is the critical point in ESD; its strength will determine most successes and failures. Packaging is the act of taking a software request and bundling the software to be delivered (with necessary installation routines, pre-installation checks, post-installation activities, and any backup that may be necessary) into a single deliverable unit. Organization should establish a set of "common" packages, which are the applications used by the entire enterprise (e.g., word processors, client shells, or standard application interfaces) or large user communities. Common packages should be distributed on a timely, well-publicized basis, typically a few times a year. The other type of package is the "exception" package (applications used by a small user population), with sporadic distribution. The goal is to minimize exception packages, as they will present the most work and cost. One minimization strategy is constantly monitoring which exceptions are requested and promoting them to the common type, therefore making them part of the resource planning and not the interrupt activity. It is also important to establish guidelines for expected delivery of exception packages (e.g., delivery can be expected one week after approval is given). Organizations should have at least one full-time person creating and testing packages Poorly created and tested packages are the leading cause of failure. If exception distributions exceed four to five per month, additional personnel will be required. Some packages will be too large to distribute over the network (typically any package above 20MB). In these cases, packages should still be created, with other media (e.g., CDs) used for distribution.

Current packaging technology is either script-driven or snapshot. Script-driven packages are essentially install programs where a script is wrapped around the application's own installation pre/post-installation routines. When using snapshot packaging, the application is installed on a test machine; a snapshot is then taken of the machines before and after appearance (e.g., which files are present; registry entries; system file or setting changes). When installing on a client, the snapshot package then reviews the client machine and adds anything else that is required to make it mirror the test machine.

Distribution

Distribution is the act of creating the list of and sending packages to the recipients. This involves sending the software directly to the end users, and the stages a package must go through in delivery. Bandwidth consumption is a consideration. To minimize this, a tool should be deployed with regional distribution hubs, where a package is delivered from a central point to the hub (over a WAN) and then replicated at the hub and distributed locally over a LAN. Distribution considerations must be taken into account when architecture designing the installations of an ESD tools. (e.g., where to locate the hubs). Distribution is not always done over the network. In cases where packages are too large, media (containing the package) should be sent to end-users. The client-side installation should still be automated, the package on the media doing as much work automatically as possible. The ESD process should plan for these cases, allowing extra time for distributions to complete. These manual distributions will normally occur with common package. Creating lists of recipients should leverage both inventory data and directory data. Inventory data should be used to identify where applications reside when doing upgrades. Directory data should be leveraged for identification of departments, groups, and other users that will all receive like applications.

Client-Side Installation

Client-side installation is the point where the software is actually laid down on a machine or target. End-user actions can cause many failures (e.g., machine turned off, not executing CD-based install), so education is required. No matter how little intervention is required by end users, they should always be notified of a distribution.

Reporting

Reporting is necessary on all packages. This should be done not just through the ESD tool itself, but also through reading the inventory database, mainly after manual packages have been sent out. Reports should also be reviewed to look for ways to improve ESD processes (e.g., identify candidates for common packages, identify significant failure patterns).

Ownership

The electronic software distribution (ESD) process will touch not only the software recipients (or end users), but also the help desk, PC support teams, application teams, and technical services teams. Any distribution should be submitted via an enterprise change management process. This process would notify all parties involved that a distribution, or change, is occurring. Managing the entire ESD process, distributing the software, monitoring end-user installations, and reporting on the process should be owned by the PC support team, as it is closest to the PC configurations. The help desk should not just be notified by the change management process, but it should also have access to the reporting system (providing data on successes and failures). It should even have the ability to distribute approved packages to fix problems. Packaging processes, the most labor-intensive, will be divided among several teams, where the full-time packaging personnel resides at the management level. Each application team should be responsible for creating and testing the packages for its given applications. However, the PC support team should package shrink-wrapped software, as this team has more knowledge of and exposure to the packages. Finally, associated technical service teams should create any server or back-office software installation or upgrade packages. The PC team should drive common packages.

- Eliminates desktop visits and human error by electronically distributing software to all desktops and servers on the network from a central location.
- Allows administrators to control application deployment and to have it occur during a specific time of day to avoid network congestion or to distribute software after certain dates to ensure users are trained first.
- Provides an installation tool that allows administrators to make changes and write scripts to custom tailor applications to their environments.

- Unattended software installation where no user interaction is needed and can be done on off-hours.
- Report on the status of distributed installations so administrators know when software was correctly installed.

Systems Management

Systems management is the coordination and management of computer systems throughout the enterprise. It includes the large mainframe systems as well as distributed systems. While the mainframe has evolved into a stable and disciplined environment, the management of distributed computing has become a more complex endeavor. This is due to the architecture and the limitations of tools to monitor and analyze this diverse environment of computer nodes, networks, and applications. Over time, network resources have become critical components for many systems and true systems management encompasses the coordination of system and network resources throughout the enterprise. Systems and network management are discussed separately in this document, but they both attempt to address many of the same issues. Critical elements such as performance, capacity, and configuration need to be incorporated into both areas. This overlap has led some to combine the discipline into a much broader category called Network/Systems Management. For our purposes, we have left them separate. We recognize that it makes sense to have a large degree of integration between the two. One cannot be managed without the other.

Systems management also includes the monitoring and management of peripheral devices and processes that are necessary for the performance, reliability, and availability of production systems. This includes such things as job scheduling, fault and event management, configuration management and security, backup and recovery, virus protection, storage management, performance and capacity monitoring, and tuning.

Asset Management

There are different management requirements for different IT and business units in an organization. It would be fair to state that there are four main constituencies that require information that use the data for different things. These groups are the CIO, the financial office, IT operations, and the Help Desk. In addition, asset management can be composed of one or more disciplines such as inventory, location, configuration, depreciation, software metering, moves/adds/changes, etc. Inventory is the key to asset management. However, it should be considered as only one piece of a more comprehensive strategy. This strategy should ultimately address the different constituency-specific applications and processes for the entire enterprise.

Repositories

Ideally, there should be one repository for all asset management data. Although this is unattainable now, it is important to understand the landscape and to position an organization to be able to retain flexibility and take advantage of products and technology. That is, to set the course for an enterprise asset management solution. To this end, there should be a goal to narrow the number of repositories. The industry is evolving toward two main repositories from the four outlined above. These boundaries can be broadly classified as finance and IT based.

The State should begin to agree on the types of information required before a consolidation of asset repositories can begin to take place.

Change Management and Other Considerations

Change management is a critical piece to an overall successful asset management strategy and implementation. Vendors are responding to this force with tighter integration between asset, change, request, and systems management. One of the primary ways to differentiate will be a vendor's ability to *link* multiple complex sources of data (e.g. help desk tickets, warranty service, actual vs. objective service levels, leasing and maintenance terms, software licensing, etc.). This will allow costs to be accurately modeled for each asset thus providing the foundation for pricing services. This software has to be balanced against cost, usefulness, convenience, and complexity.

There are benefits of integrating asset management into the help desk. The most obvious is instant access to desktop attributes. However, as the help desk evolves and the first call resolution becomes a greater issue at the help desk, it is important for the help desk to be informed of all the changes and financial ramifications of assets. The ability to understand that certain changes may be impacting problems at the help desk is an essential component to an integrated help desk.

The asset management process flow, or asset life-cycle processes, can be broadly summarized as follows: procurement, installation, move/add/change, support, maintenance, and disposal. It is very important to have an integrated change and service request system that also addresses ad hoc service requests and technical refreshes. Asset tracking, in itself, is not a single process, but a component of various life-cycle processes. Any event that touches an asset has the potential to corrupt the state of where an asset is and how it is configured. Presently, there is no single tool available to accomplish what is outlined here.

Network Management Platforms

Network management platforms should assist network operators during the network life cycle. The platform should be flexible and provide an "open-ended" approach to business solutions.

The network management system should be cross platform capable of running on various platforms including UNIX and Windows NT, and provide the same capabilities on either platform. Provide an "open ended" platform capable of working with third party software for additional hardware and software application solutions. The system should be capable of managing computer hardware prevalent at the State such as CISCO routers, Cabletron hubs, American Power Supply UPSs, and other hardware platforms.

Software and hardware support 7x24 for technical questions is necessary as well as providing automatic software updates to the network management system. Provide setup and installation of system as well as formal and informal training.

Domain Principles

The following principles are provided to guide the State of Connecticut in the evaluation, selection, design, construction, implementation and management of the products and services within the Enterprise Systems Management Domain.

Business Oriented Principles

Information Is an Enterprise Asset

Information is valued as an enterprise asset, which must be shared to enhance and accelerate decision making.

Justification

- Enhances the efficiency and effectiveness of the delivery of services.
- Most information is in isolated pockets such that the value of information is not always recognized.
- Enables new enterprise-wide solutions.
- Treating the data as an enterprise asset increases its integrity and relevance of data.

Implications

- Need to develop policy pertaining to information stewardship.
- Information value must be identified, authenticated, and leveraged.
- Need to establish supporting policies for security, privacy, confidentiality and information sharing.
- Data needs to be structured for easy access and management.

Architecture Management

The planning and management of the State's enterprise-wide technical architecture *must be unified* and *have a planned evolution that is governed across the enterprise.*

Justification

- Without a unified approach, there will be multiple, and possibly conflicting, architectures.
- Good change requires collaboration and collective planning.
- Architecture must be well thought out.
- Governance will be simplified.

Implications

- A unified approach will require a change in cultural attributes.
- Normal evolution will require prioritization and reprioritization across all IT initiatives.
- Dependencies must be maintained.

- The architecture must be continually re-examined and refreshed.
- Short-term results vs. long term impact must be constantly considered.
- Establishing enterprise architecture takes time and involves a lot of change.

Architecture Compliance

Architecture support and review structures shall be used to ensure that the integrity of the architecture is maintained as systems and infrastructure are acquired, developed and enhanced.

Justification

- To realize the benefits of a standards-based enterprise architecture, all information technology investments must ensure compliance with the established IT architecture.
- For maximum impact, review should begin as early in the solution planning process as possible
- "If you are going to talk the talk, then you must be willing to walk the walk."

Implications

- A structured project level review process will be needed to ensure that information systems comply with the IT Architecture and related standards.
- Processes incorporating the principles of this (technical) architecture must be developed for all application procurement, development, design, and management activities.
- This compliance process must allow for the introduction of new technology and standards.
- Principle should be used as evaluation criteria for purchasing as well as developing software.

Ensure Security, Confidentiality and Privacy

Systems Management systems should be implemented in adherence with all security, confidentiality and privacy policies and applicable statutes.

Justification

- Helps to safeguard confidential and proprietary information
- Helps to ensure the integrity of the information

Implications

- Need to identify, publish and keep the applicable policies current
- Need to monitor compliance to policies
- Must make the requirements for security, confidentiality and privacy clear to everyone.
- Education on issues of privacy and confidentiality must become a routine part of normal business processes.

Reduce Integration Complexity

The enterprise architecture should try to reduce integration complexity to the most feasible extent possible.

Justification

- Increases the ability of the enterprise to adapt and change.
- Reduces product and support costs

Implications

- Decreases the number of vendors, products, and configurations in the State's environment.
- Must maintain configuration discipline.
- Will sacrifice performance and functionality in some instances.
- Will rely on components supplied by vendors.

Re-use before Buying, Buy before Building

We will consider re-use of existing applications, systems, and infrastructure before investing in new solutions. We will use / build only those applications or systems that will provide clear business advantages and demonstrable cost savings

Justification

- Use and availability of effective packaged solutions is increasing.
- Using tested solutions reduces risks.
- Reduces the total cost of ownership.

Implications

- "The definition of "reusable" will include solutions available from other government entities (e.g., other states, federal government, etc.).
- Areas that provide clear advantages and businesses cost savings are likely to require quick adaptation.
- Must identify the areas in which the State is seeking to distinguish itself.

Integration

Systems must be designed, acquired, developed, or enhanced such that data and processes can be shared and integrated across the enterprise and with our partners.

Justification

- Increase efficiency while better serving our customers (e.g., the public, agencies, etc.).
- Redundant systems cause higher support costs.
- Ensures more accurate information, one that has a more familiar look and feel.
- Integration leads to better decision making and accountability.

Implication

- IT staff will need to consider the impacts on an enterprise wide scale when designing applications.
- We will need new tools and training for their proper use.

- Will need a method for identifying data and processes that need integration, when integration should take place, whom should have access to the data, and cost justification for integration.
- Will need a “coordinator” that can maintain and arbitrate a common set of domain tables, data definitions, and processes across the organization.
- Over integration can lead to difficult data management and inefficient processes.

Reengineer First

New information systems will be implemented after business processes have been analyzed, simplified or otherwise redesigned as appropriate.

Justification

- Work processes will be more streamlined efficient and cost effective.
- Work processes, activities, and associated business rules will be well understood and documented.
- Reduces the total cost of ownership.

Implications

- Need to have an agreed upon business re-engineering process
- New technology will be applied in conjunction with business process review.
- Business processes must be optimized to align with business drivers.
- Additional time and resources will have to be invested in analysis early in the systems life cycle.
- Organizational change will be required to implement reengineered work processes.

Total Cost of Ownership

Adopt a total cost of ownership model for applications and technologies which balances the costs of development, support, training, disaster recovery and retirement against the costs of flexibility, scalability, ease of use, and reduction of integration complexity.

Justification

- Leads to higher quality solutions.
- Enables improved planning and budget decision-making.
- Reduces the IT skills required for support of obsolete systems or old standards.
- Simplifies the IT environment.

Implications

- The State budget process needs to accommodate Total Cost of Ownership of a system over a longer timeframe than current budgeting models.
- Will require looking closely at technical and user training costs especially when making platform or major software upgrades during the lifetime of the system.
- Requires designers and developers to take a systemic view.

- Need to selectively sub-optimize individual IT components.
- Need to develop a cost of ownership model.
- Need to ensure coordinated retirements of systems.

Minimize Platform Configurations

Create a small number of consistent configurations for deployment across the enterprise.

Justification

- The cost of IT personnel is increasing and the cost of hardware is decreasing rapidly, *i.e.*, “Ride the hardware cost curve”.
- This is the most efficient approach to enterprise-wide infrastructure configuration and maintenance.
- By constantly ‘tweaking’ the performance of an individual server or desktop computer, a multitude of unique configurations is created, thus increasing support and maintenance costs.
- Standardized decisions in product selection simplifies training, learning curve and skills transfer.

Implications

- Increased initial capital investment.
- Deploy applications on uniformly configured servers (“If in doubt, use the bigger Box”).
- Plan to replace multiple, non-standard, configurations with a small number of consistent configurations.
- Plan for the regular replacement of platform components to ensure the retirement of obsolete and unique configurations.

Technology Principles

The following principles guide the design and selection of Enterprise Systems Management technology components that will support computing activities across the State:

Limit the number of permutations in products

Rationale:

Organizations should limit the number of permutations in products to facilitate support efforts and reduce long-term support costs. For every additional permutation of a deployed product, there is a corresponding increase in complexity and costs to support the different permutation.

Minimize "unique" performance tuning requirements

Rationale:

Performance tuning for unique/non-standard components is not worth the increased maintenance costs of multiple configurations. Performance tuning can inhibit change by encouraging comfort with the status quo. It’s much more cost effective to find an equivalent supported product that meets the functionality required by such a “unique” solution.

Selected tools must support the definition of reliable metrics and provide reports for proactive Enterprise Systems Management

Rationale:

Reliable metrics and reports must be defined and used to assist managers, help desk staff, and the client community to assess the effectiveness of the help desk in meeting organizational goals. Both consolidated high level and low level detailed measures are critical to successful service desk operations. Monitoring system information and trend analysis of performance statistics for comparing system operations generates important information necessary to remotely support each of the domains and their sub-components monitored by Enterprise Systems Management. Metrics should be used and supported by each particular tool to identify trends and to support a proactive management approach that anticipates and avoids problems

Maintain configuration inventories in real time

Rationale:

Inventories of hardware and software configurations should be maintained by, or be available to the help desk, network operations center staff and other Enterprise Systems Management and ISD support team members. Such information should include all physical components (processor, RAM, disk drive, network cards, add-on cards) and other types of relevant information.

Any selected Enterprise Systems Management software should provide some linkage to inventory management. Examples could include the use of inventory ‘agents’ or applications that survey and record current inventory facilitate collection from desktops and servers.

Enterprise Systems Management solutions shall encompass support for remote Enterprise Systems Management

Some examples of remote Enterprise Systems Management services include:

- Backup, archiving and recovery
- System, database and application monitoring
- Software distribution to the server and/or desktop

Implications:

There are two inferences from this principle:

- Enterprise Systems Management solutions must provide remote access and authentication from systems that are not dedicated to the Enterprise Systems Management solution. For example, an engineer who receives a support call at home should be able to dial-in, check the status and take any corrective actions that the system allows, remotely.
- For systems that are remote (i.e., not physically connected to the systems at the State), the tools should support the management of the remote system when connected to the network, regardless of connection method.

Selected solutions shall limit customer responsibilities for Enterprise Systems Management

Similar to the requirement for remote Enterprise Systems Management, this principle reinforces the concept and tightens the requirement by recognizing the costs for THE STATE to provide competent staff to perform such functions at remote locations.

Rationale:

Therefore, although the equipment may be located close to the business community, local user efforts should be concentrated on performing their business functions rather than on system management tasks such as system configuration, debugging and/or backup.

Design for advance notice of failure

System components should *proactively* ALERT in advance of failure including predictive capability.

Rationale:

System generated alarms and alerts should be automatically routed to the appropriate Enterprise Systems Management resource. For example:

- Database problems should be routed to the database support group.
- PC hardware problems should be routed to PC support.
- Agents should be able to issue alerts for both hardware and applications.

Disaster recovery and backup solutions protect server, application and data integrity

Rationale:

Although, at times, it may be important to reduce the points of failure in a deployed solution, it is much more important to provide disaster recovery services in case of a complete failure. It is the responsibility of this domain to ensure that the State can continue to operate any solution given a reasonable SLA (negotiated between the business and ISD). The domain should be able to provide such a solution for any given server, application or data set.

Enterprise Systems Management tools shall support the monitoring and measuring of capacity (inventory), systems reliability (uptime), system stability and accessibility

Rationale:

Recognizing that there may be different tools for managing different solutions, it is still important to seek consistency for selected tool sets. The common area of consistency is in providing proactive solutions for these purposes.

Business Continuity Oriented Principles

Mainstream Technologies

IT solutions will use industry-proven, mainstream technologies.

Justification

- Avoids dependence on weak vendors.
- Reduces risk.
- Ensures robust product support.
- Enables greater use of commercial-off-the-shelf solutions.

Implications

- Need to establish criteria for vendor selection and performance measurement.
- Need to establish criteria to identify the weak vendors and poor technology solutions.
- Requires migration away from existing weak products in the technology portfolio.

Industry Standards

Priority will be given to products adhering to industry standards and open architecture.

Justification

- Avoids dependence on weak vendors.
- Reduces risks.
- Ensures robust product support.
- Enables greater use of Commercial-off-the-Shelf solutions.
- Allows flexibility and adaptability in product replacement.

Implications

- Requires a culture shift
- Need to establish criteria to identify standards and the products using them.
- IT organizations will need to determine how they will transition to this mode.

Disaster Recovery / Business Continuity

An assessment of business recovery requirements is mandatory when acquiring, developing, enhancing or outsourcing systems. Based on that assessment, appropriate disaster recovery and business continuity planning, design and testing will take place.

Justification

- Due to factors such as the Internet and Y2K, customers and partners have heightened awareness of systems availability.
- The pressure to maintain availability will increase in importance. Any significant visible loss of system stability could negatively impact our image.
- Continuation of business activities without IT is becoming harder.
- Application systems and data are valuable State assets that must be protected.

Implications

- Systems will need to be categorized according to business recovery needs (e.g. business critical, non-critical, not required).

- Alternate computing capabilities need to be in place.
- Systems should be designed with fault tolerance and recovery in mind.
- Plans for work site recovery will need to be in place.
- Costs may be higher.

Scalability

The underlying technology infrastructure and applications must be scalable in size, capacity, and functionality to meet changing business and technical requirements.

Justification

- The Total Cost of Ownership is minimized.
- Encourages reuse.
- Leverages the continuing decline in hardware costs.

Implications

- Scalability must be reviewed for both “upward” and “downward” capability.
- May increase initial costs of development and deployment.
- Will reduce some solution choices.

Domain Standards

Introduction

The Platform Architecture Principles illustrate the need to reduce the hardware and software configuration of platforms and operating systems supported by DOIT. This will increase flexibility, reduce costs, increase reuse, and build on existing skill sets. The standards reflect the current state of the infrastructure at the State of Connecticut. These standards are based on a point in time snapshot of the existing State of Connecticut IT infrastructure. These standards will provide a level-set foundation for future technology investments that assist in meeting the principles. These standards will be used as the State of Connecticut's Information Technology Systems mature and should be viewed as a migration path for existing platforms and as the target platforms for new systems. Platform technology will be periodically evaluated for a possible refresh of the existing standards.

We have classified the technology as follows:

Obsolete

It is highly likely that these standards or products, while still in use, will not be supported by the vendor (industry, manufacturer, etc.) in the future. Some products and standards have already reached the non-supported state. Plans should be developed by the agencies or the State to rapidly phase out and replace them with strategic standards or products. No development should be undertaken using these standards or products by either the agencies or the State.

Transitional

These are standards or products in which an agency or the State has a substantial investment or deployment. These standards and products are currently supported by DOIT, the agencies, or the vendor (industry, manufacturer, etc.). However, agencies should undertake development using these standards or products only if there are no suitable alternatives that are categorized as strategic. Plans should be developed by the agencies or the State to move from transitional to strategic standards or products as soon as practical. In addition, the State should not use these standards or products for development.
Note: many older versions of *strategic* standards or products fall into this category, even if not specifically listed in a domain architecture document.

Strategic

These are the standards and products selected by the state for development or acquisition, and for replacement of *obsolete* or *transitional* standards or products. (Strategic means a three to four year planning horizon.) When more than one similar strategic standard or product is specified for a technology category, there may be a preference for use in statewide or multi-agency development. These preferred standards and products are indicated where appropriate.
Note: some strategic products may be in “pilot testing” evaluation to determine implementation issues and guidelines. Pilot testing must be successfully completed prior to full deployment by the agencies or the State.

Research / Emerging

This category represents proposed strategic standards and products that are in advanced stages of development and that should be evaluated by the State. The some of these standards or products may already be undergoing "hands-on" evaluation. Others will need to be tracked and evaluated over the next 6 to 18 months.

Technology Components (Products)

Table 1 Enterprise Systems Mangement Product Standards

	Status Category			
Product Existing or Proposed	Obsolete	Transitional	Strategic	Research
Help Desk problem ticketing, tracking etc.				
Impact		✓		
NMS9300 (Notes Based)	✓			
Help Star 2000		✓		
Track-IT				✓
Help Trac				✓
Royal Blue				✓
Asset Management				
Impact		✓		
Track-IT				✓
LanDesk		✓		
Royal Blue				✓
Remote Monitoring Desktop/Server systems management				
NetView				✓
OpenView		✓		
Managewise		✓		

	Status Category			
Product Existing or Proposed	Obsolete	Transitional	Strategic	Research
Remote Monitoring Desktop/Server systems management (cont.)				
Zenworks		✓		
Control-IT (was Remotely Possible)		✓		
Performance Works		✓		
What's Up Gold			✓	
WebTrends			✓	
Site Scope		✓		
MS-Zac		✓		
MS-SMS		✓		
Next Point		✓		
Network Systems Management				
NetView 6000			✓	
OpenView		✓		
Managewise		✓		
Zenworks		✓		
Control-IT (was Remotely Possible)		✓		
Cabletron Spell		✓		
Ether Peak		✓		
Router PM			✓	
Cisco Works			✓	

	Status Category			
Product Existing or Proposed	Obsolete	Transitional	Strategic	Research
Network Systems Management cont.				
Fluke Network Inspector			✓	
Next Point		✓		
Remote Monitoring mainframe systems management				
Omagamon			✓	
NetView for OS/390			✓	
TMON			✓	
Software Distribution				
Zenworks				✓
MS-SMS				✓
Veritas/Winistall				✓
ZAK		✓		
Ghost		✓		
lotus Notes		✓		
HP SW Distributor		✓		
Tivoli				✓
CA				✓
Cisco Works			✓	

Technology Standards

The following standards have been established to support operational systems management for the enterprise. As new and/or revised standards emerge, they will be documented in a future release of this section. Standards reflect the current state of the infrastructure at the State. It's important to note that infrastructure is only a representation of the architecture at a point in time.

The infrastructure may or may not reflect the future state envisioned by the principles, but it does provide a leverage point for future technology investments that assist in meeting the principles.

Standard 1: SNMP protocols

The Simple Network Management Protocol (SNMP) is a collection of Internet protocols. These protocols are the standard for managing TCP/IP based networks. It is built into the devices (concentrators, routers etc.) in the network and in the network operating systems of the servers and workstations. The network management system uses SNMP to collect statistics and other information on network devices. SNMP is also used to send commands that control the State network devices. SNMPv2, simply called SNMP, is the recommended standard.

Standard 2: RMON products

Remote Monitoring (RMON) products are used in most enterprise networks. RMON products provide packet collection, decoding and analysis to the MAC layer of the Operating Systems Interconnection (OSI) stack using a combination of consoles and hardware and software probes that relied on SNMP MIB data collections. In 1992, the Internet Engineering Task Force, IETF, specified the RMON1 standard in RCF 1271. The RMON1 MIB extends SNMP capability by monitoring sub-network operation and reducing the data collection burden on management consoles and network agents. The RMON2 standard was approved by the IETF in January, 1997 in RCF2021. RMON2 includes a new MIB to extend network monitoring into the application-monitoring layer. RMON functionality is growing to include functions like applications monitoring, report generation and bandwidth allocation. All the major vendors of network devices have added RMON MIB collection capability to their products, although the depth of implementation relative to the full RMON specification varies among vendors and products.

Standard 3: DMI standard

The Desktop Management Interface (DMI) standard was developed by the DeskTop Management Task Force (DMTF) which sets specifications for the management of the desktop environment. The DMI is a set of API's that allow different vendor applications to consistently share the desktop. It sets the standard for a management platform that enables a common standardized mechanism for Enterprise Systems Management of the desktop while permitting vendor differentiation. As vendors build desktops with embedded DMI standards, important desktop management information will become available.

Standard 4: Web-Based Enterprise Management (WBEM)

Standard 5: Java Management API (JMAPI)

Internet technologies are being employed more and more in the area of systems management. The two main technical solutions are:

1) Web-Based Enterprise Management (WBEM) which is backed by Microsoft, Intel, and Compaq

2) Java Management API (JMAPI) backed by Sun.

The use of web technologies in the field of information systems management offers certain advantages. First, the use of a universal interface (i.e. browser) helps administrators to be more mobile since information can be accessed from any machine equipped with a browser. Second, there is a reduced development time, particularly the eventual elimination of porting administrative applications to different platforms. Third, improved services offered in the interface, in the agent (more intelligent agent), and in the application (with the emergence of Internet/intranet applications in the enterprise, it is easy to develop links with web management applications).

Network Management Platforms

Tools for the platform should include but not be limited to:

Topology Discovery – Platform should provide for automatic discovery of devices and network topology. Be capable of controlling the scope of discovery and recognize various vendor specific devices (e.g., Cisco Routers, Cabletron Hubs). Provide various configurable "Views" of networks with administrative control of display handling for security and users requirements.

Network Monitoring – Provide automatic and active monitoring of all devices and connections through out the network. Graphically display status of network devices and connections through color-coded status indicators. Provide automatic change of status indicators.

Configuration Database – Provides network topology configuration and device inventory in database format. Provide utilities to export database to other database or file formats (e.g., UDB, Oracle). Provide full database platform with utilities to control and manage database.

Trouble Ticket System – Provides a trouble ticket system to actively display, log and report network related problems as they occur and is capable of filtering events to appropriate displays.

Event Handling – Provide automatic handling of network related events as they occur. Provides trap handling and notification with capabilities of sending traps to other systems. Capable of Email notification, beeper notification, auto correcting procedures when events occur. This capability should be provided in an easy to use GUI interface.

Data Collection / Reporting – Provide capabilities for data collection on various types of networking equipment. Provide built in applications for reporting network performance statistics in a friendly GUI form. Capability to customize reports for specific reporting needs. Capable of printing and displaying graphs and reports through a web interface.

Help Desk Best Practices

Client/server based help desk applications and related software packages are necessary to support help desk business functions. These applications record and track events, automate event queue and event escalation, support development of event history and resolution knowledge bases, facilitate reporting, and promote integration with other support functions such as change and service management.

The following practices are recommended to develop a **service oriented** help desk.

1. **The help desk and user support functions must be re-engineered to provide an integrated support services environment.**
   - The central help desk provides the focal point to mediate problems.
   - Support tools should empower both the help desk analyst and the end user with self-help capabilities.
2. **The help desk should actively work to improve the perception of its services within the organization.**

   Help desk analysts must be empowered to take ownership of problems and given the tools to solve them.

   - As part of managing the changing perception of the help desk organization, marketing events, such as newsletters, should target the end-user community as well as their managers.
   - Upper management should periodically work on the help desk to demonstrate commitment to service and gain greater appreciation for user needs.
   - Training for end users should be included in all plans for the improvement of help desks.
3. **In order to provide the best customer service environment, it may be necessary to elevate and/or restructure the help desk within the organization.**
   - The help desk organization should be elevated in the organizational and reporting structure to operate unencumbered by other units, making customer service needs its top priority.
   - The role of the help desk analyst is changing. Help desk staff should serve on project teams, and participate in training, application design, testing, and maintenance.
   - All requests for service should be channeled through the help desk when feasible.
4. **A single consolidated help desk design supports an enterprise model.**
   - A consolidated help desk does not have to be physically located in one place. However, it should have one constituency, one phone number, one set of procedures, one set of defined services, and one set of integrated network systems management platforms and applications.

The implementation of the virtual data center (VDC), where many remote LANs are managed as a single entity, supports the corresponding development of consolidated help desk services.

5. **Each centralized help desk unit must provide a single point of contact (SPOC).**
   - A SPOC minimizes user inconvenience and confusion. In its broadest sense, SPOC means that the end user makes one attempt at contact and the help desk request is channeled by some automated means to the organization that can best service the request.
   - The help desk should mediate all problems.
6. **In order to leverage support resources and provide effective client support, multiple tiers or levels of client support are required.**

- Tier/Level 1 client support should have end-to-end responsibility for each client request. The help desk analyst should be empowered to resolve as many requests as possible. Tier 1 provides the client contact point (CCP) or call ownership, which is the single point of contact for the end user to request a service. Organizations should retain control of the Tier 1 help desk in order to ensure the quality of the customer relationship.
- Tier/Level 2 client support provides advanced technical expertise to the tier/level 1 client contact points. Their responsibility is to analyze the requests routed to them and resolve the problems. Resources at this level can be composed of staff specialists and/or third party providers/vendors.
- Tier/Level 3 support is composed of highly specialized technical experts. Calls, which cannot be solved at tiers/levels 1 and 2, are routed to this level. Resources at this level can be composed of staff specialists and/or third-party providers/vendors.

7. **Reliable metrics and reports must be defined and used to assist managers, help desk staff, and the client community to assess the effectiveness of the help desk in meeting organizational goals.**
   - Both consolidated high level and low level detailed measures are critical to successful service desk operations.
   - Metrics should be used to identify trends and to support a proactive management approach that anticipates and avoids problems.
   - Monitoring server information and trend analysis of performance statistics for comparing LAN operations generates important information necessary to remotely support many LANs.
   - Methods and procedures to solve problems should be developed, published, followed, and measured.
   - Service Level Agreements (SLAs) should be developed stating responsibilities of both the help desk and its clients. SLA criteria are one method to evaluate help desk performance.
8. **Geographically dispersed help desk units must inter-operate and share information.**
   - All requests for service should reside in a database that is shared by technology and application-based help desk units that serving specific constituencies throughout the state. This process shares information and makes it possible for one help desk to electronically pass a service request to another help desk without forcing the user to make another contact attempt.
   - The use of technological advances, such as distributed processing, dynamic control of users desktop, improved telephony, and client support software, make it possible for geographically dispersed help desk groups to function as a cohesive support unit.
9. **Resolution databases that contain solutions to recurring problems should be built to improve service quality and contain costs.**
   - Building and using a knowledge base of prior resolutions to solve problems improves the quality of resolutions.

- Help desk operations should include problem resolution links to external systems.

10. The help desk should maintain inventories of hardware and software configurations.

They should include all physical components (processor, RAM, disk drive, network cards, add-on cards) and other types of relevant information.

- Current inventories are critical to support functions.
- Inventory “agents” or applications that survey and record current inventory facilitate collection from desktops and servers.

Gaps (or To Be Determined)

The Enterprise Systems Management space is broad in scope and contains key elements that are critical to continued successful operations of State IT operations. Their importance become more apparent as systems and infrastructure expand which is issues of scalability and complexity. This makes examination of this topic a daunting task. After the first iteration of the EWTA process there are significant gaps that exist. The next step is to address these gaps.

Technology Components

The domain team needs to be re-examined and refined the entire section on technology components. The original list consists of a large percentage of the products that were a result of the statewide inventory that was conducted. We were reluctant to remove products that may have been incorrectly categorized in the first pass. For example, there are some products listed that really are tools and utilities that are important in the day-to-day execution of IT activities. There were not classified or considered as transitional or strategic products.

In only a few cases have we indicated that there are products outside our current installed base that need to be considered (e.g., for example, CA and Tivoli in the Software Distribution area). There needs to be a concerted effort in the next phase to examine what is available and appropriate beyond what we have currently listed.

The status categories assignments themselves will need to be analyzed again with an eye towards eliminating or decreasing (through research) the research category. A gap associated with this process is the amount of time and resources available to conduct a proper analysis.

Best Practices and Guidelines

The level of integration and interoperability between products and product suites is something that must be examined. It is discussed in this document, but will be examined and understood in detail. One essential component related to this is the investment the State has in both product and experience in certain products and product suites. It is not clear as to how this relates to everything else in the technology component space. How will these products perform future requirements, degree of modification, upgrade, or change that will be required? How well they interface and complement other essential products in the other categories?

IT Policies

There needs to be an examination of missing and outdated policies. In addition, there should be a more complete examination and better documentation of de facto standards and policies. One example of this would be in the storage area. Presently there are efforts underway to refine and articulate enterprise-wide storage and backup strategies. This includes traditional methods of storage as well as Storage Area Networks and Network Attached Storage. Also included are appropriate backup and recovery methodologies and technologies for the appropriate storage space. These efforts need to be included into the EWTA process.

Help Desk

In the current system, a hotline call is received into the data center. The person answering the call then determines if it can be handle by them or the call is routed to the area to handle the issue. The problem is that current system does not track in any form the cause, nature or resolution of the problem. There is no vendor database or interface to better contact or dispatch hardware technicians to fix the problem. There currently is no system that helps to identify where user education would help cut down on hotline calls. The current system cannot route the problem to a specific person or area where the situation can be handled in a timely manner. A database based system with links to E-mail and System Monitoring packages are already standard on the market today. To better maximize personnel and time an Automated system to handle the Help Desk/ Hotline needs to be implemented.